

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

SYMANTEC CORPORATION,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. _____
	)	
ZSCALER, INC.,	)	<b>JURY TRIAL DEMANDED</b>
	)	
Defendant.	)	

**COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiff Symantec Corporation (“Symantec” or “Plaintiff”) files this complaint for patent infringement against Defendant Zscaler, Inc. (“Zscaler” or “Defendant”) and in support thereof alleges and avers as follows:

**NATURE OF THE ACTION**

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq.*, specifically including 35 U.S.C. § 271.

**THE PARTIES**

2. Symantec is a corporation organized under the laws of the State of Delaware, with a principal place of business at 350 Ellis Street, Mountain View, California.

3. On information and belief, Zscaler is a corporation organized under the laws of the State of Delaware, with a principal place of business at 110 Rose Orchard Way, San Jose, California.

### **JURISDICTION AND VENUE**

4. This Court has subject matter jurisdiction over this patent infringement action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler regularly transacts business in Delaware, including but not necessarily limited to offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware. Accordingly, this Court may properly exercise personal jurisdiction over Zscaler.

6. Venue lies in this judicial district pursuant to 28 U.S.C. §§ 1391(b), 1391(c) and/or 1400(b) at least because Zscaler is deemed to reside in this judicial district by virtue of being incorporated in the State of Delaware. In addition, on information and belief, Zscaler has committed acts of infringement in the State of Delaware, including but not necessarily limited to offering products or services that infringe one or more of Symantec's asserted patents to customers located in Delaware and/or for use in Delaware.

### **THE PATENTS-IN-SUIT**

7. U.S. Patent No. 6,285,658 ("the '658 Patent"), titled "System for Managing Flow Bandwidth Utilization at Network, Transport and Application Layers in Store and Forward Network," was issued by the United States Patent and Trademark Office ("USPTO") on Sept. 4, 2001. Symantec is the owner by assignment of the entire right, title and interest in and to the '658 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '658 Patent is attached hereto as Exhibit A.

8. U.S. Patent No. 7,360,249 (“the ’249 Patent”), titled “Refining Behavioral Detections for Early Blocking of Malicious Code,” was issued by the USPTO on Apr. 15, 2008. Symantec is the owner by assignment of the entire right, title and interest in and to the ’249 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’249 Patent is attached hereto as Exhibit B.

9. U.S. Patent No. 7,587,488 (“the ’488 Patent”), titled “Dynamic Background Rater for Internet Content,” was issued by the USPTO on Sept. 8, 2009. Symantec is the owner by assignment of the entire right, title and interest in and to the ’488 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’488 Patent is attached hereto as Exhibit C.

10. U.S. Patent No. 8,316,429 (“the ’429 Patent”), titled “Methods and Systems for Obtaining URL Filtering Information,” was issued by the USPTO on Nov. 20, 2012. Symantec is the owner by assignment of the entire right, title and interest in and to the ’429 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’429 Patent is attached hereto as Exhibit D.

11. U.S. Patent No. 8,316,446 (“the ’446 Patent”), titled “Methods and Apparatus for Blocking Unwanted Software Downloads,” was issued by the USPTO on Nov. 20, 2012. Symantec is the owner by assignment of the entire right, title and interest in and to the ’446 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the ’446 Patent is attached hereto as Exhibit E.

12. U.S. Patent No. 8,402,540 (“the ’540 Patent”), titled “Systems and Methods for Processing Data Flows,” was issued by the USPTO on March 19, 2013. Symantec is the owner by assignment of the entire right, title, and interest in and to the ’540 Patent, including the sole

and undivided right to sue for infringement. A true and correct copy of the '540 Patent is attached hereto as Exhibit F.

13. U.S. Patent No. 9,525,696 ("the '696 Patent"), titled "Systems and Methods for Processing Data Flows," was issued by the USPTO on Dec. 20, 2016. Symantec is the owner by assignment of the entire right, title, and interest in and to the '696 Patent, including the sole and undivided right to sue for infringement. A true and correct copy of the '696 Patent is attached hereto as G.

14. The '658 Patent, '249 Patent, '488 Patent, '429 Patent, '446 Patent, '540 Patent, and '696 Patent are referred to herein collectively as the Patents-in-Suit.

### **BACKGROUND OF THE DISPUTE**

#### **Symantec Is a Pioneer in Fundamental Networking and Security Technology**

15. Since its inception, Symantec has been providing software products to enhance its customers' computing productivity, security and reliability. Symantec was founded in 1982 by computer scientist Gary Hendrix with a grant from the National Science Foundation. Originally focused on natural language processing and artificial intelligence-related products, Symantec grew throughout the 1980s through organic growth and strategic acquisitions in the computer software field. In 1990, Symantec merged with Peter Norton Computing, a developer of various consumer antivirus and data management utilities. At the time, Symantec was already a market leader for Macintosh antivirus and utilities software and had already begun development of a DOS-based antivirus program, making the merger with Norton strategically advantageous. Norton AntiVirus was launched in 1991. In 1993, the Norton product group accounted for 82% of Symantec's total revenues.

16. Among other areas of expansion, Symantec sought to develop and acquire more products for corporate customers. Specifically, Symantec sought to offer products that would serve enterprise environments in which desktop computers were connected with local and other networks. Symantec was determined to achieve a goal of providing integrated, platform independent and centralized network administration solutions. Symantec's investment and innovation led to the launching the Norton Enterprise Framework in 1996. By the late 1990s, Symantec was marketing three major product lines. The first line covered security and assistance products, consisting mainly of Norton AntiVirus and Norton Utilities products to keep personal computers protected and reliable. The second line included remote productivity solutions, which enabled telecommuters, mobile professionals and workers in remote offices to access information, applications and data on-demand from any location. The third line included internet tools, primarily for Java programmers.

17. On August 1, 2016, Symantec acquired Blue Coat Systems, Inc. ("Blue Coat"). Blue Coat was founded in 1996, and has been a leading provider of advanced web security solutions for global enterprises and governments. Through the acquisition, Symantec expanded and complemented its technology offerings with the addition of Blue Coat's security platform technology.

18. Symantec (including Blue Coat) has been a market leader with its technology offerings and has been dedicated to continued innovation to help customers secure and manage their information. Symantec expended tremendous resources in research and development to create the intellectual property upon which its products are based. Over the years, Symantec has invested billions of dollars in research and development, and a significant portion of that investment is protected by a portfolio of over 2,000 United States patents.

**Zscaler's Infringing Cloud Security Platform**

19. Zscaler is a relative newcomer to the network security arena, having been founded in 2008. Zscaler has gained momentum in the marketplace through unlawful use of the technology claimed in the Patents-in-Suit. Symantec is a direct competitor with Zscaler in the network security space, and Zscaler's infringement of the Patents-in-Suit is causing Symantec irreparable harm.

20. On information and belief, Zscaler's cloud security platform, including without limitation its Zscaler Enforcement Node or "ZEN" component (collectively, "the Zscaler Platform"), infringes one or more of the Patents-in-Suit, as described in more detail below.

**PATENT INFRINGEMENT CLAIMS**

**Count I – Infringement of U.S. Patent No. 6,285,658**

21. Symantec incorporates by reference the allegations in Paragraphs 1 through 20 above.

22. The '658 Patent is generally directed to bandwidth control of Internet Protocol (IP) flows according to detected selectable information about an IP flow. *See* '658 Patent, 1:57-60.

23. On information and belief, Zscaler directly infringes one or more claims of the '658 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

24. Claim 7 of the '658 Patent recites as follows:

A method for managing bandwidth on Internet Protocol (IP) flows in a packet communication environment allocated into layers, including at least a transport layer, a link layer and an application layer, said method comprising:

automatically detecting selectable information about each one of said flows;

determining a policy for assigning a service level to said flows based upon said selectable information automatically detected about one of said flows; and

implementing said policy by explicit data rate control of said one of said flows.

25. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 7. Zscaler's cloud security platform, including its ZEN component, performs a method for managing bandwidth on Internet Protocol (IP) flows in a packet communication environment allocated into layers, including at least a transport layer, a link layer and an application layer. For example, Zscaler provides bandwidth control features that allow for management of bandwidth on IP flows, such as by allocating bandwidth to certain applications or by throttling bandwidth. Zscaler performs this method in a packet communication environment by communicating packets over the Internet between an Internet host and a client. That environment includes a transport layer, a link layer, and an application layer. Zscaler's cloud security platform, including its ZEN component, automatically detects selectable information about each one of the flows by, for example, determining that a particular flow is associated with an application class or URL. Zscaler offers seven predefined classes of business applications, including general surfing, large files, sales/support applications, financial applications, media/streaming, web conferencing, and voice over IP. Zscaler's cloud security platform, including its ZEN component, determines a policy for assigning a service level to the flows based upon said selectable information automatically detected about one of the flows. For example, ZScaler's platform includes policies for certain URLs or traffic classes. Whenever the ZEN is analyzing traffic, the ZEN determines if the traffic meets any of the policy's URLs or traffic classes. When the ZEN identifies a match, the ZEN associates the URL or traffic class

with the service level (e.g., guaranteeing bandwidth or throttling bandwidth) that's been assigned to that traffic class or URL. Zscaler's cloud security platform, including its ZEN component, implements the policy by explicit data rate control of said one of said flows by, for example, throttling bandwidth or guaranteeing a minimum bandwidth.

26. In view of the foregoing, Zscaler directly infringes the '658 Patent in violation of 35 U.S.C. § 271(a).

27. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '658 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '658 Patent, Zscaler is inducing infringement of the '658 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '658 Patent.

28. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count II – Infringement of U.S. Patent No. 7,360,249**

29. Symantec incorporates by reference the allegations in Paragraphs 1 through 28 above.

30. The '249 Patent is generally directed detecting and blocking attempted malicious behavior of running code. *See* '249 Patent, Abstract.

31. On information and belief, Zscaler directly infringes one or more claims of the '249 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such

infringement are provided below, based on the limited information currently available to Symantec.

32. Claim 12 of the '249 Patent recites as follows:

A computer implemented method for preventing malicious code from propagating in a computer, the method comprising the steps of:

a blocking-scanning manager detecting attempted malicious behavior of running code;

responsive to the detection, the blocking-scanning manager blocking the attempted malicious behavior;

the blocking-scanning manager generating a signature to identify the code that attempted the malicious behavior, wherein generating a signature to identify the code that attempted the malicious behavior comprises:

the blocking-scanning manager applying a hash function to generate a hash of the code that attempted the malicious behavior; the blocking-scanning manager storing the hash; and

the blocking-scanning manager using at least one stored hash to identify code that attempted malicious behavior; the blocking-scanning manager detecting code identified by the signature; and the blocking-scanning manager blocking the execution of the identified code.

33. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 12. ZScaler's cloud security platform, including its ZEN component and its Behavior Analysis functionality prevents malicious code from propagating in a computer, as described below. ZScaler's cloud security platform, including its ZEN component, includes a blocking-scanning manager detecting attempted malicious behavior of running code. For example, ZScaler's Behavior Analysis functionality executes suspicious files in a sandbox, analyzes them for malicious behavior, and detects malware files. ZScaler's cloud security platform, including its ZEN component, includes: responsive to the detection, the blocking-scanning manager blocking the attempted malicious behavior. For example, Zscaler's Behavior

Analysis functionality automatically blocks malware files; further, some files are quarantined until the behavioral analysis is complete and then blocked after quarantining. ZScaler's cloud security platform, including its ZEN component, includes the blocking-scanning manager. The blocking-scanning manager generates a signature to identify the code that attempted the malicious behavior. The generation of a signature to identify the code that attempted the malicious behavior includes the blocking-scanning manager applying a hash function to generate a hash of the code that attempted the malicious behavior and the blocking-scanning manager storing the hash. For example, the Zscaler platform runs and analyzes files in a virtual environment to detect malicious behavior and propagates a hash of malicious files to Zscaler ZENs to maintain a blacklist against downloading malicious files. ZScaler's cloud security platform, including its ZEN component, includes the blocking-scanning manager using at least one stored hash to identify code that attempted malicious behavior, the blocking-scanning manager detecting code identified by the signature, and the blocking-scanning manager blocking the execution of the identified code. For example, Zscaler's platform, including its ZEN component, allegedly effectively maintains a real time blacklist so it can prevent users anywhere in the world from downloading malicious files.

34. In view of the foregoing, Zscaler directly infringes the '249 Patent in violation of 35 U.S.C. § 271(a).

35. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '249 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '249 Patent, Zscaler is inducing infringement of the '249 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of

service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '249 Patent.

36. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count III – Infringement of U.S. Patent No. 7,587,488**

37. Symantec incorporates by reference the allegations in Paragraphs 1 through 36 above.

38. The '488 Patent is generally directed to dynamically generating Internet-content ratings. *See* '488 Patent, 1:14-18.

39. On information and belief, Zscaler directly infringes one or more claims of the '488 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

40. Claim 1 of the '488 Patent recites as follows:

At a computer system, a method for dispatching an Internet-content identifier to a content-rating system, the method comprising:

receiving an indication that at least one unrated Internet-content identifier is available to be rated;

receiving an indication that one or more computerized content raters are available for rating the at least one unrated Internet-content identifier, wherein the computerized content raters include a plurality of content classifiers configured to rate content based on respective criteria;

selecting an Internet-content identifier from among the at least one unrated Internet-content identifier based on content-identifier selection criteria;

selecting one computerized content rater from among the one or more available computerized content raters to rate the selected unrated Internet-content identifier;

transferring the selected Internet-content identifier to the selected available computerized content rater, wherein the selected Internet-content identifier identifies a portion of content; and

dynamically determining a content category rating for the selected Internet-content identifier, wherein determining a content category rating comprises dynamically combining a rating for the selected Internet-content identifier with at least one of a rating for an Internet-content identifier identified within the portion of content for the selected Internet-content identifier and an Internet-content identifier for a portion of content that identifies the selected Internet-content identifier.

41. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 1. ZScaler's cloud security platform, including its ZEN component, dispatches an Internet-content identifier to a content-rating system. For example, the Page Risk Index feature of Zscaler's cloud security platform rates a URL, as described below. ZScaler's cloud security platform, including its ZEN component, receives an indication that at least one unrated Internet-content identifier is available to be rated. For example, the Page Risk Index feature of Zscaler's cloud security platform receives a new request to rate a URL. ZScaler's cloud security platform, including its ZEN component, receives an indication that one or more computerized content raters are available for rating the at least one unrated Internet-content identifier, wherein the computerized content raters include a plurality of content classifiers configured to rate content based on respective criteria. For example, the Page Risk Index feature uses Content Analysis and Domain Analysis control categories, each with various risk categories, and the Page Risk Index feature is calculated for each and every web request. ZScaler's cloud security platform, including its ZEN component, selects an Internet-content identifier from among the at least one unrated Internet-content identifiers based on content-identifier selection criteria. For example, ZScaler's cloud security platform, including its ZEN

component, scans every web request and selects a URL to rate. ZScaler's cloud security platform selects one computerized content rater from among the one or more available computerized content raters to rate the selected unrated Internet-content identifier. For example, ZScaler's cloud security platform routes traffic to a particular ZEN component running the Page Risk Index feature. ZScaler's cloud security platform transfers the selected Internet-content identifier to the selected available computerized content rater, wherein the selected Internet-content identifier identifies a portion of content. For example, ZScaler's cloud security platform, including its ZEN component, calculates a page risk index for each and every web request. The URL is transferred to the selected available computerized content rater when the request is made and/or the page risk index calculated, and the URL identifies a portion of content. ZScaler's cloud security platform, including its ZEN component, dynamically determines a content category rating for the selected Internet-content identifier, wherein determining a content category rating comprises dynamically combining a rating for the selected Internet-content identifier with at least one of a rating for an Internet-content identifier identified within the portion of content for the selected Internet-content identifier and an Internet-content identifier for a portion of content that identifies the selected Internet-content identifier. For example, ZScaler's cloud security platform, including its ZEN component, dynamically determines a page risk index for a particular web request (URL). The determined page risk index is based on a weighting of a variety of risk indicators, including injected content where page content is inspected to identify code injected into a web page, designed to directly initiate a browser attack or redirect the browser to an alternate page hosting malicious content.

42. In view of the foregoing, ZScaler directly infringes the '488 Patent in violation of 35 U.S.C. § 271(a).

43. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '488 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '488 Patent, Zscaler is inducing infringement of the '488 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '488 Patent.

44. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count IV – Infringement of U.S. Patent No. 8,316,429**

45. Symantec incorporates by reference the allegations in Paragraphs 1 through 44 above.

46. The '429 Patent is generally directed to policing secure socket layer (SSL) encrypted traffic according to a content category of an Internet host (e.g., a URL). *See* '429 Patent, 2:4-6; 3:25-29.

47. On information and belief, Zscaler directly infringes one or more claims of the '429 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

48. Claim 1 of the '429 Patent recites as follows:

A method, comprising:

receiving, at a proxy, a client hello message from a client;

transmitting, from said proxy to an Internet host, a request for a digital certificate associated with the Internet host;

extracting, at the proxy, information from the digital certificate associated with the Internet host;

categorizing, at the proxy, said Internet host into one or more content categories according to said information extracted from the digital certificate, said categorizing including maintaining a table at said proxy wherein each Internet host is associated with a category which defines attributes of the Internet host or content associated with the Internet host; and

based on the one or more content categories into which the Internet host is categorized, determining, at the proxy, whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet host so as to permit examination of the encrypted communication at the proxy.

49. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 1. Zscaler's cloud security platform, including its ZEN component, receive, at a proxy (e.g., a ZEN), a client hello message from a client. For example, Zscaler's ZEN component receives a client hello message from a client (e.g., a subscriber's computer) in the form of an HTTPS request from the client. Zscaler's cloud security platform, including its ZEN component, transmit, from the proxy to an Internet host, a request for a digital certificate associated with the Internet host. For example, Zscaler's ZEN component transmits an HTTPS request to a destination server thereby initiating an SSL handshake. Zscaler's cloud security platform, including its ZEN component, extracts information from the digital certificate associated with the Internet host. For example, Zscaler's ZEN component receives a certificate from the destination server and reads information from the certificate during validation of the destination server. Zscaler's cloud security platform, including its ZEN component, categorizes the Internet host into one or more content categories according to the information extracted from the digital certificate. For example, Zscaler's ZEN component categorizes URLs into various

different classes, supercategories, and categories consistent with information extracted from the destination server's certificate. Zscaler's cloud security platform, including its ZEN component, maintains a table at the proxy wherein each Internet host is associated with a category that defines attributes of the Internet host or content associated with the Internet host. For example, Zscaler's cloud security platform includes a table for each class, supercategory, and category that associates URLs with particular categories. The categories further include attributes that define the Internet host or content associated with the host, such as a description of the "gambling" category that defines attributes of "gambling" sites as "sites that provide online gambling or are related to gambling assistance, training, information, or advocacy." Zscaler's cloud security platform, including its ZEN component, based on the one or more content categories into which the Internet host is categorized, determines whether to (i) pass encrypted communication between a client and the Internet host through the proxy without decrypting the encrypted communication at the proxy or (ii) decrypt the encrypted communication between the client and the Internet host so as to permit examination of the encrypted communication at the proxy. For example, Zscaler's cloud security platform permits SSL configuration such that SSL communications that fall within certain URL categories are passed from the destination server to the client through the ZEN without decrypting the communication. If the SSL communication does not fall within one of the specified URL categories, then the communication is decrypted so that the ZEN can inspect the decrypted communication for, among other things, data leakage, malicious content, viruses, and to enforce policy. As such, the ZEN determines whether to pass the encrypted SSL communication or decrypt the communication based on the categorization of URLs into content categories.

50. In view of the foregoing, Zscaler directly infringes the '429 Patent in violation of 35 U.S.C. § 271(a).

51. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '429 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '429 Patent, Zscaler is inducing infringement of the '429 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '429 Patent.

52. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count V – Infringement of U.S. Patent No. 8,316,446**

53. Symantec incorporates by reference the allegations in Paragraphs 1 through 52 above.

54. The '446 Patent is generally directed to preventing the unwanted download and installation of malicious code on a computer. *See* '446 Patent, 1:41-42; Abstract.

55. On information and belief, Zscaler directly infringes one or more claims of the '446 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

56. Claim 1 of the '446 Patent recites as follows:

A method, comprising:

intercepting at a Uniform Resource Locator (URL) filter module of a network device, an attempted download of a file from a URL;

categorizing by the URL filter module of the network device the URL into a URL category according to a URL database;

analyzing by a file type identifier module of the network device the file to determine its file type, wherein the file type of the file is determined by detecting one or more of a file type signature in the file and a file extension of the file, and identifying the file type of the file based on one or more of the file type signature detected in the file and the file extension of the file; and

blocking or not blocking the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type, wherein (i) if the URL category indicates a blacklist, the decision output is to block the download, (ii) if the URL category indicates a whitelist, the decision output is to allow the download, otherwise, the URL category specifies a URL content category indicating a type of content provided by the URL, and the decision output is based on whether files of said file type are permitted for URLs in the URL content category.

57. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of Claim 1. Zscaler's cloud security platform, including its ZEN component, intercepts at a Uniform Resource Locator (URL) filter module of a network device, an attempted download of a file from a URL. For example, Zscaler's ZEN component inspects files being returned from an Internet host (e.g., www.google.com) to a client. Zscaler's cloud security platform, including its ZEN component, categorizes by the URL filter module of the network device the URL into a URL category according to a URL database. For example, Zscaler's ZEN categorizes URLs into URL categories (e.g., the classes, supercategories, or categories used in URL filtering) according to a URL database (e.g., the global URL category database). Zscaler's cloud security platform, including its ZEN component and its File Type Analysis module, analyzes by a file type identifier module of the network device the file to determine its file type, wherein the file type of the file is determined by detecting one or more of a file type signature in the file and a file extension of the file. For example, Zscaler's ZEN component analyzes files,

such as attachments to e-mails or HTTP transactions, to detect the file type (e.g., executable, Office document, archive file, image, audio, video, etc.) by scanning the files to determine the file extension (e.g., .exe, .scr, etc.). Zscaler's cloud security platform, including its ZEN component, identifies the file type of the file based on one or more of the file type signature detected in the file and the file extension of the file. As discussed above, for example, Zscaler's ZEN identifies file type by scanning a file to determine the file's extension. Zscaler's cloud security platform, including its ZEN component, blocks or does not block the attempted download according to a decision output of a blocking decision module of the network device which receives as inputs the URL category and the file type. As noted above, for example, the Zscaler's ZEN knows a URL category and a file type. The ZEN will output a decision that either blocks or does not block an attempted download. If the ZEN's File Type Policy specifies a URL category as a blacklist, the ZEN's decision is to block the download. For example, the ZEN may block particular types of files within the webmail URL category if the URL is blacklisted. Alternatively, the ZEN's File Type Policy may indicate that the URL category is whitelisted and not block the download. Otherwise, the URL category specifies a URL content category indicating a type of content provided by the URL, and the decision output is based on whether files of said file type are permitted for URLs in the URL content category. Zscaler utilizes URL content categories in the form of classes, supercategories, and categories. For example, Zscaler utilizes a class of legal liability, a supercategory of adult material, and a category of adult themes. If the File Type Policy does not specify that the file type is allowed or blocked for a particular URL category, the ZEN determines if files of the particular file type are permitted for URLs in the particular URL content category. For example, if no File Type Policy is specified for executable files downloaded from adult themed websites, the ZEN determines whether to block or allow the download based on whether downloading executable files is permitted for URLs within the adult themed URL content category.

58. In view of the foregoing, Zscaler directly infringes the '446 Patent in violation of 35 U.S.C. § 271(a).

59. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '446 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '446 Patent, Zscaler is inducing infringement of the '446 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '446 Patent.

60. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count VI – Infringement of U.S. Patent No. 8,402,540**

61. Symantec incorporates by reference the allegations in Paragraphs 1 through 60 above.

62. The '540 Patent is generally directed to processing data flows to ensure application of a security policy. *See* '540 Patent, Abstract.

63. On information and belief, Zscaler directly infringes one or more claims of the '540 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

64. Claim 13 of the '540 Patent recites as follows:

A virtualized network security system (VNSS) comprising:

a plurality of flow processing facilities configured as elements of the VNSS for processing a data flow, said data flow being transferred between a first port and a second port of the VNSS, the data flow comprising subscriber profile data;

a network management facility that is networked with the plurality of flow processing facilities; and

a first security policy for a first virtual network, based at least in part on the subscriber profile data included in the data flow;

a second security policy for a second virtual network, based at least in part on the subscriber profile data included in the data flow, wherein the two or more flow processing facilities receive at least one of the first security policy and the second security policy while receiving said data flow on said plurality of first ports and transferring said data flow to said plurality of second ports,

wherein the plurality of flow processing facilities make a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data; and

wherein the plurality of flow processing facilities make a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data.

65. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of at least Claim 13. Zscaler's cloud security platform, including its ZEN component, implements policy enforcement by providing a VNSS. For example, Zscaler's cloud security platform creates a global network that acts as a single virtual proxy. Zscaler's cloud security platform, including its ZEN component, includes a plurality of flow processing facilities that are configured as elements of the VNSS for processing a data flow, and the data flow is transferred between a first port and a second port of the VNSS. As an example, Zscaler's ZEN component uses multiple security analysis engines to analyze traffic. Once traffic reaches the ZEN component, the security analysis engines scan the content using, for example, Zscaler's ByteScan technology. Zscaler's cloud security platform, including its ZEN component, also

includes a network management facility that is networked with the plurality of flow processing facilities. As an example, Zscaler's cloud security platform, including its CA component, communicates with the ZEN component and directs traffic to the ZEN component. Zscaler's cloud security platform, including its ZEN component, includes a first security policy for a first virtual network, which is based at least in part on the subscriber profile data included in the data flow, and also includes a second security policy for a second virtual network, based at least in part on the subscriber profile data included in the data flow. For example, Zscaler's cloud security platform, including its ZEN component, supports group and user policies being provisioned on the Zscaler database to enable Zscaler's cloud security platform, including its ZEN component, to authenticate the user. Enabling authentication allows Zscaler's cloud security platform, including the ZEN component, to identify the traffic that it receives so it can enforce the configured group and user policies. Zscaler's cloud security platform, including its ZEN component, also enforces policies with user-level granularity based on defining the policies according to a user or a group. Zscaler's cloud security platform, including the ZEN component, includes two or more flow processing facilities that receive at least one of the first security policy and the second security policy while receiving the data flow on the plurality of first ports and transferring the data flow to the plurality of second ports. For example, Zscaler's cloud security platform, including its ZEN component, receives the content and enforces the security policies served by the CA to implement the group and user policies. Zscaler's cloud security platform includes multiple ZEN components, and the ZEN component includes multiple security analysis engines that scan the content according to the security policies. Zscaler's cloud security platform, including the ZEN component, include the plurality of flow processing facilities to make a first determination, in accordance with one of the first security policy and the second

security policy, of abnormalities that are associated with the data flow. For example, Zscaler's cloud security platform, including its ZEN component, uses Zscaler's ByteScan technology to inspect every byte of a request, content, responses, and all related data for inline blocking threats like viruses, cross site scripting, and botnets. As another example, Zscaler's cloud security platform, including its ZEN component, inspects all end user traffic through Single Scan Multi Action technology to ensure security against current and emerging threats based on the user provisioning. Single Scan Multi Action technology subjects the content to every level of inspection unless malicious content is identified at a lower level. Using Zscaler's cloud security platform, including its ZEN component, the first determination is based at least in part on the subscriber identified by the subscriber profile data. The plurality of flow processing facilities makes a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data. As an example, Zscaler's cloud security platform, including its ZEN component, inspects every byte of traffic inline across multiple security techniques and enforces compliance according to granular user policies. Zscaler's cloud security platform may be configured to enforce multiple security policies, including, but not limited to, web security, advanced threats, and anti-virus and anti-spyware.

66. In view of the foregoing, Zscaler directly infringes the '540 Patent in violation of 35 U.S.C. § 271(a).

67. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '540 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '540 Patent, Zscaler is inducing infringement of the '540 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of

service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '540 Patent.

68. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**Count VII – Infringement of U.S. Patent No. 9,525,696**

69. Symantec incorporates by reference the allegations in Paragraphs 1 through 68 above.

70. The '696 Patent is generally directed to processing data flows to provide security and protection to a computer. *See* '696 Patent, Abstract.

71. On information and belief, Zscaler directly infringes one or more claims of the '696 Patent, either literally or under the doctrine of equivalents. Non-limiting examples of such infringement are provided below, based on the limited information currently available to Symantec.

72. Claim 1 of the '696 Patent recites as follows:

A flow processing facility for implementing a security policy, comprising:

a plurality of application processing hardware modules, each configured with an application for processing data packets;

a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets; and

a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile and for transmitting the identified data packets in at least one of series and parallel to the identified application processing modules based on the security policy.

73. On information and belief, the Zscaler cloud security platform satisfies each and every limitation of at least Claim 1. Zscaler's cloud security platform, including its ZEN component, implements policy enforcement by providing a flow processing facility for implementing a security policy. For example, the Zscaler platform is a complete security platform that supports security policies. Zscaler's cloud security platform, including its ZEN component, includes a plurality of application processing hardware modules, and each is configured with an application for processing data packets. As an example, Zscaler's ZEN component analyzes traffic using multiple security analysis engines. Once traffic reaches the ZEN component, the security analysis engines scan the content through, for example, Zscaler's ByteScan technology. Zscaler's cloud security platform, including its ZEN component, also includes a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets. For example, Zscaler's cloud security platform, including its ZEN component, supports group and user policies being provisioned on the Zscaler database to enable Zscaler's cloud security platform, including its ZEN component, to authenticate the user. Enabling authentication allows Zscaler's cloud security platform, including the ZEN component, to identify the traffic that it receives so it can enforce the configured group and user policies. Zscaler's cloud security platform, including its ZEN component, includes a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile. As an example, Zscaler's cloud security platform, including its Central Authority (CA) component, directs traffic to the ZEN component based on the user's location and ensures that the policy is applied according to the user's location, device, application, or content through context-aware security. The ZEN

component implements Zscaler's Single Scan Multiple Action technology to accurately identify the application to use for processing the content. Zscaler's cloud security platform, including its ZEN component, includes the network processing module that transmits the identified data packets in at least one of series and parallel to the identified application processing modules based on the security policy. For example, Zscaler's cloud security platform, including the CA component, directs the traffic to the ZEN component, and the ZEN component implements Single Scan Multiple Action technology to identify the security analysis engines to scan the content.

74. In view of the foregoing, Zscaler directly infringes the '696 Patent in violation of 35 U.S.C. § 271(a).

75. On information and belief, both by configuring the ZEN component to operate in a manner that Zscaler knows infringes the '696 Patent and by encouraging customers to use the ZEN component in a manner that Zscaler knows infringes the '696 Patent, Zscaler is inducing infringement of the '696 Patent by its customers in violation of 35 U.S.C. § 271(b), at least as of service of this complaint. For example, Zscaler's marketing literature touts functionality of the ZEN component that falls within the scope of the above-identified claims of the '696 Patent.

76. Symantec has no adequate remedy at law for Zscaler's acts of infringement. As a direct and proximate result of Zscaler's acts of infringement, Symantec has suffered and continues to suffer damages and irreparable harm. Unless Zscaler's acts of infringement are enjoined by this Court, Symantec will continue to be damaged and irreparably harmed.

**PRAYER FOR RELIEF**

WHEREFORE, Symantec prays for judgment in its favor granting the following relief:

- A. A finding that Zscaler has directly infringed and/or induced others to infringe the Patents-in-Suit;
- B. An award of damages pursuant to 35 U.S.C. § 284 adequate to compensate Symantec for Zscaler's infringement of the Patents-in-Suit, including both pre- and post-judgment interest and costs as fixed by the Court;
- C. A preliminary and/or permanent injunction against Zscaler and its officers, agents, servants, employees, and representatives, and all others in active concert or participation with them, from further infringing the Patents-in-Suit;
- D. A declaration that this is an exceptional case within the meaning of 35 U.S.C. § 285, and a corresponding award of Symantec's reasonable attorney fees incurred in connection with the litigation; and
- E. Any additional and further relief the Court may deem just and proper under the circumstances.

**JURY DEMAND**

Pursuant to Federal Rule of Civil Procedure 38(b) and District of Delaware Local Rule 38.1, Plaintiff hereby demands a trial by jury on all issues so triable.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Jeremy A. Tigan

Jack B. Blumenfeld (#1014)  
Jeremy A. Tigan (#5239)  
1201 North Market Street  
P.O. Box 1347  
Wilmington, DE 19899-1347  
(302) 658-9200  
jblumenfeld@mnat.com  
jtigan@mnat.com

*Attorneys for Plaintiff Symantec Corporation*

OF COUNSEL:

Kurt Pankratz  
Chad Walters  
BAKER BOTTS LLP  
2001 Ross Avenue  
Dallas, TX 75201

Jennifer C. Tempesta  
BAKER BOTTS LLP  
30 Rockefeller Plaza  
New York, NY 10112  
(212) 408-2571

April 18, 2017  
10976004